

CLAIMS

Please cancel claims 9 and 18-20 without prejudice and enter new claims 33-40.

Claims 1-32 (Canceled)

33. (New) A method for performing an initial handshake during secure communications in a computer network comprising:

coupling a client to a web server;

generating a public/private key pair at the web server by:

generating prime numbers r_1 and r_2 ;

generating N by multiplying r_1 and r_2 ;

selecting arbitrary numbers p and q ;

generating d such that $d = r_1 \bmod (p-1)$ and also $d = r_2 \bmod (q-1)$; and

calculating e' by multiplying d^{-1} and $\bmod \phi(N)$ whereby the public key is $[N, e']$ and the private key is $[r_1, r_2]$;

using the public key to encrypt a pre-master secret R such that the encrypted pre-master secret R is a secret encrypted C , at the client;

sending the secret encrypted C to the web server from the client;

receiving the secret encrypted C at the web server;

decrypting the secret encrypted C to obtain the encrypted pre-master secret R at the web server; and

using the encrypted pre-master secret R to establish a session encryption key.

34. (New) The method as recited in claim 33 wherein the secure communications include Secure Socket Layer ("SSL") messages.

35. (New) The method as recited in claim 33 wherein the secure communications include Transport Layer Security ("TLS") messages.

36. (New) The method as recited in claim 33 wherein the secure communications include Internet protocol secure ("IPSec") messages.

37. (New) A method for performing an initial handshake during secure communications in a computer network comprising:

coupling a client to a web server;

generating a public/private key pair at the web server based upon a selection of a pair of prime numbers and a pair of arbitrarily selected numbers;

using the public key to encrypt a pre-master secret R such that the encrypted pre-master secret R is a secret encrypted C, at the client;

sending the secret encrypted C to the web server from the client;

receiving the secret encrypted C at the web server;

decrypting the secret encrypted C to obtain the encrypted pre-master secret R at the web server; and

using the encrypted pre-master secret R to establish a session encryption key.

38. (New) The method as recited in claim 37 wherein the secure communications include Secure Socket Layer ("SSL") messages.

39. (New) The method as recited in claim 37 wherein the secure communications include Transport Layer Security ("TLS") messages.

40. (New) The method as recited in claim 37 wherein the secure communications include Internet protocol secure ("IPSec") messages.